ABSTRACT OF THE DISCLOSURE

Provided is an elliptic curve exponentiation apparatus that can counter the DFA when an elliptic curve exponentiation technique is used. A computation result verification unit 127 receives, as a computation result, an exponentiation-result-point (X, Y) from an elliptic curve computation unit 124. The computation result verification unit 127 computes $X^3+a\times X+b$, and computes Y^2, and outputs the received exponentiation-result-point when judging that $Y^2=X^3+a \times X+b$, and does not output the received exponentiation-result-point when not judging that $Y^2=X^3+a \times X+b$.

(Selected Figure) FIG. 3